REMARKS

Claims 1-6, 8-10, and 12-20 were pending in the application. Claims 8, 10, and 12 have been cancelled. Claims 1, 4-5, 13-15, and 18 have been amended. The figures have been amended to correct a reference designation. No new matter has been added. Claims 1-6, 9, and 13-20 remain pending in the application. Reconsideration is respectfully requested in view of the amendments to the claims and the following remarks.

I. Response to Amendment

While Applicant acknowledges that the Examiner has provided a definition of the term "map" as determined by the Oxford English Dictionary Online, the Examiner is respectfully reminded that an Applicant is entitled to be his or her own lexicographer. See *In re Paulsen*, 30 F.3d 1475, 1480, 31 USPQ2d 1671, 1674 (Fed. Cir. 1994). As noted by the Examiner, claims are interpreted in light of the specification, and therefore the term "map" cannot be construed to be such that it would be contrary to the Applicant's specification.

II. Claim Objections

Claims 1-6, 8-10, and 12-20 were objected to based on a number of informalities, each of which is addressed below.

Applicant has amended the preamble of claim 1 to recite "a computer-implemented method for encrypting and decrypting" so that the scope of the preamble is consistent with the scope of the body of the claim. Applicant has further deleted "presenting the decrypting original string for processing" from claim 1. With respect to the phrase "a processor-implemented method", Applicant has amended the phrase to read

"a computer-implemented method" which is supported in the specification, for example, in paragraphs [0032]-[0033] and FIG. 1. In addition, Applicant has included a limitation of "using an encryption equation to map the original string to an encrypted string" consistent with paragraph [0026] of the specification. Applicant has also amended claim 1 to include other limitations – e.g., mapping the original string to an encrypted string and using factor decryption equations - as suggested by the Examiner.

Each of independent claims 15 and 18 have been amended similar to claim 1 to address the Examiner's objections.

Applicant therefore respectfully requests withdrawal of the objections to the claims.

III. The § 112 Rejections

Claims 1-6, 8-10, and 12-20 were rejected under 35 U.S.C. § 112, first paragraph, as containing subject matter which was not described in the specification in such a way to enable one skilled in the art to make the invention.

Claims 1-6, 8-10, and 12-20 were also rejected under 35 U.S.C. § 112, second paragraph, as being indefinite.

Applicant has amended each of claims 1, 15, and 18 to correspond with the specification.

Applicant, therefore, respectfully requests withdrawal of the § 112 rejections.

IV. The § 101 Rejections

Claims 15-17 were rejected under 35 U.S.C. § 101 as being directed towards non-statutory subject matter.

Claims 15-17 have been amended to include a processor, and a memory in communication with the processor. The memory stores instructions that are executable by the processor for implementing the limitations as recited in claim 15.

Claims 18-20 were further rejected under 35 U.S.C. § 101 as being directed towards non-statutory subject matter. Applicant has amended claims 18-20 to recite computer readable medium claims that are statutory. That is, "computer readable medium" claims are recognized as an accepted type of claim, similar to "method," "system," and "device" claims. Specifically, MPEP § 2106 states:

> [A] claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory.

(M.P.E.P. § 2106.IV.B.1(a), 8th ed., 4th rev.)

Therefore, based on the reasons above, Applicant respectfully requests withdrawal of the § 101 rejections.

V. The § 103 Rejections

Claims 1-6, 8-10, and 12-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,677,952 to Blakely, III et al. ("Blakely"). Applicant respectfully traverses the rejections.

Claim 1, as amended, recites a computer-implemented method for encrypting and decrypting an original string that is storable in a database. In particular, the method includes storing a false derivative value in the database, in which the false derivative value is used to determine a given factor from a set of factors during decryption of a stored encrypted string.

A. *Blakely Fails To Disclose* Storing *a False Derivative Value in a Database, in which the False Derivative Value is used to Determine a Given Factor from a Set of Factors During Decryption of a Stored Encrypted String*

Blakely discloses a method for protecting information in a storage disk of a computer using a secret key (see Abstract). The method includes applying a length-increasing pseudorandom function to the secret key and an index to generate a pseudorandom bit string (having a length that is a function of the size of a sector of a disk). The pseudorandom bit string is then used to encrypt and decrypt data accesses to and from the sector (col. 2, ll. 10-18). In one aspect, the secret key is preprocessed by transforming the secret key into one or more tables of pseudorandom numbers (an "efficient representation" of the secret key) (col. 2, ll. 33-35). The one or more tables of pseudorandom numbers are supplied to the length-increasing pseudorandom function to generate the pseudorandom bit string (col. 5, ll. 31-40).

The Examiner recognizes that Blakely fails to disclose false derivative values. However, the Examiner has associated "false derivative values" to "pseudorandom numbers" stored within the one or more tables of pseudorandom numbers, and asserts that only a set of values from the table of pseudorandom numbers is used to generate the pseudorandom bit string. The Examiner then concludes therefore that it would have been obvious to one of skill in that a set of the values in the table of pseudorandom numbers are false derivative values that are not used during decryption.

Applicant respectfully disagrees with the Examiner's assertion that not all of the pseudorandom numbers stored within the table of pseudorandom numbers are not used during decryption. As described in column 8, lines 3-24, **multiple iterations** are

performed during generation of the pseudorandom bit sequence. Consequently, after all iterations have been processed – all of the values within the table of pseudorandom numbers (i.e., the "efficient representation" of the secret key) are used. Thus, the pseudorandom numbers stored within the table of pseudorandom numbers cannot read on false derivative values as recited in claim 1.

For at least these reasons, Applicant submits that claim 1, and the claims that depend therefrom, are allowable over Blakely.

B. *Other Independent Claims*

Claims 15 and 18 each incorporates limitations similar to those of claim 1. Claims 15 and 18 (and the claims that depend therefrom) are also allowable over Blakely for reasons corresponding to those set forth with respect to claim 1.

Should any unresolved issues remain, the Examiner is invited to call the undersigned at the telephone number indicated below.

Respectfully submitted,
SAWYER LAW GROUP LLP

August 23, 2007
Date

/Kelvin M. Vivian/
Kelvin M. Vivian
Attorney for Applicant
Reg. No. 53,727
(650) 475-1448